

White Paper

# Microsoft EOP + IRONSCALES = a Complete Email Security Solution

Leverage the Microsoft Licenses You Already Own





## Introduction

A truly effective email security solution should include both spam filtering and advanced phishing protection. Your existing Microsoft E1/E3 licenses include Exchange Online Protection (EOP), which does a fantastic job at filtering out spam. EOP paired with the advanced phishing protection provided by IRONSCALES will provide you with a complete email security solution without the need to purchase more expensive E5 license from Microsoft or to have to rely on other Secure Email Gateway technologies for spam filtering capabilities.

This document is intended to support your decision to utilize IRONSCALES while recognizing that you require a smooth pathway to transition your Spam filtering technology. We have identified a transition strategy and specific configuration steps to maximize the utilization of your existing Microsoft licenses and capabilities. The goal to help transition Spam services away from your Secure Email Gateway to a commoditized solution that you already have access to but may not be fully utilizing yet.



# Contents

---

Challenge .....	4
A Strategy For Navigating Organizational Challenges .....	4
Configure Anti-spam Policies in EOP.....	6
Prerequisite .....	6
Use The Security Center to Create Anti-Spam Policies.....	7
Wrapping Up.....	19

## Challenge

While the combination of EOP + IRONSCALES has been proven to be an effective email solution from a technology perspective, as an IT leader you are likely to face a number of other organizational challenges and pushback.

## A Strategy For Navigating Organizational Challenges

Based on experiences we have had with many customers who were once where you are, we put together this guide to help you successfully navigate the minefield of internal organizational challenges to ultimately arrive at what we feel (and our customers have stated) is the optimal solution for a Microsoft E1/E3 license owner when it comes to email security.



### Overcommunicate

Overcommunicate what change you are making (a transition to commercialized Spam Controls), why you are making this change (extracting extra value from tools you're already paying for), when you are making this change, and how individuals can quickly receive support.



### Lead From the Front

The IT organization and team members should make the switch first so they understand any potential impact and what to expect. Collect feedback and quickly document any concerns that may have materialized. Share these documents with your support team, make sure they know where to find this information quickly as needed.



### Prepare Your Team

Ensure your support team(s) and/or helpdesk are aware of the transition, support paths, common questions/concerns they may encounter, and how to respond appropriately.



### Focus on VIPs

Start with VIPs of your organization, once you successfully transition these folks, you will face far fewer obstacles later. As concerns get raised to these leaders, they will be able to reference their own successful experience and help their teams see the value and support this organizational change.

- With VIPs, we encourage taking a white glove approach. Have the VIP support path(s) communicated in advance personally (an email alone will likely NOT be effective). If possible, identify a 'war room' type location where VIPs can go immediately where support will be available.
- If the number of VIPs are very large, consider implementing only a few VIP 'waves' at a time. Those who are resistant to change should be mixed with early adopters. Divide the waves up based on your unique knowledge of the team, but do not concentrate select personalities in one wave (i.e., do not put all your highly-resistant-to-change leaders in one wave).



### Start to Scale

Scale up the waves for the remainder of the organization. With the VIP leaders on board, now you want to transition to larger groups. If you have many physical sites, **break up the waves by function**, not location. If you group waves based on location alone, the local support team will become overwhelmed, and local leadership could become resistant to this change, undermining the hard work you did with VIPs previously..



### Finish Strong!

Continually add waves to the transition until complete. Remember, the objective of a successful wave is to prevent significant business disruption. Please expect users to object or question these changes, change is always hard, this behavior are humans doing human things. Continually focus on the goal: to make the transition as quickly as possible with the least amount of disruption or consternation within your business cycle.



## Configure Anti-Spam Policies In EOP

In Microsoft 365 organizations with mailboxes in Exchange Online or standalone Exchange Online Protection (EOP) organizations without Exchange Online mailboxes, inbound email messages are automatically protected against spam by EOP, which uses anti-spam policies (also known as spam filter policies or content filter policies) as part of your organization's overall defenses against spam.

The basic elements of an anti-spam policy are:

- **The spam filter policy:** Specifies the actions for spam filtering verdicts and the notification options.
- **The spam filter rule:** Specifies the priority and recipient filters (who the policy applies to) for a spam filter policy.

## Prerequisite

You need to be assigned permissions in Exchange Online before you can do the procedures in this article:

- To add, modify, and delete anti-spam policies, you need to be a member of the **Organization Management** or **Security Administrator** role groups.
- For read-only access to anti-spam policies, you need to be a member of the **Global Reader** or **Security Reader** role groups.

**Anti-spam technologies in EOP:** <https://security.microsoft.com/antispam>

Configure policies that are included in anti-spam protection. These policies include connection filtering, spam filtering, outbound spam filtering, and spoof intelligence.

Microsoft 365 Defender

Policies & rules > Threat policies > Anti-spam policies

Use this page to configure policies that are included in anti-spam protection. These policies include connection filtering, spam filtering, outbound spam filtering, and spoof intelligence. [Learn more](#)

+ Create policy Refresh 3 items Search

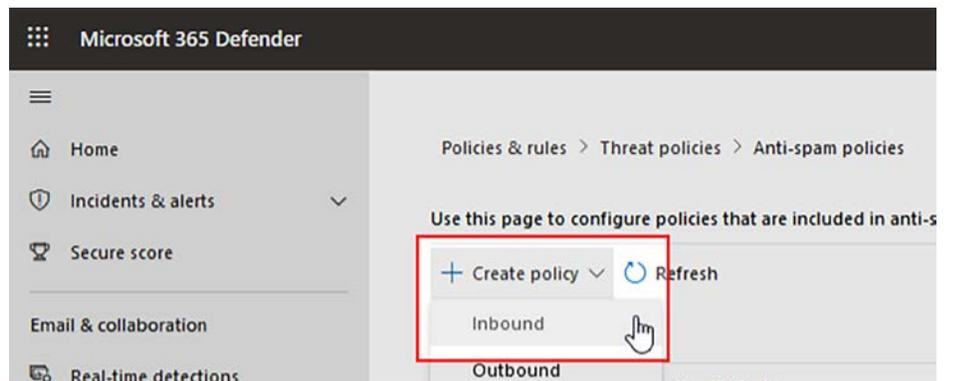
Name	Status	Priority	Type
Anti-spam inbound policy (Default)	Always on	Lowest	
Connection filter policy (Default)	Always on	Lowest	
Anti-spam outbound policy (Default)	Always on	Lowest	

## Use The Security Center To Create Anti-Spam Policies

Creating a custom anti-spam policy in the security centre creates the spam filter rule and the associated spam filter policy at the same time using the same name for both.

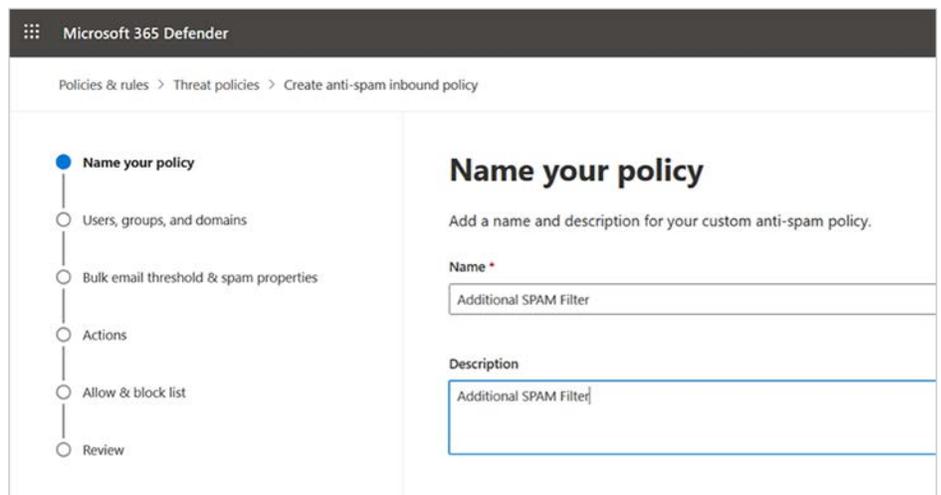
Go to [Anti-spam policies](#)

- 1 On the Anti-spam policies page, click **+Create policy** and then select **Inbound** from the drop-down list.



- 2 The policy wizard opens. On the **Name your policy** page, configure these settings:

- **Name:** Enter a unique, descriptive name for the policy.
- **Description:** Enter an optional description for the policy.



When you are finished, click **Next**.

3

On the **Users, groups, and domains** page that appears, identify the internal recipients that the policy applies to (recipient conditions):



### Users

The specified mailboxes, mail users, or mail contacts in your organization.



### Groups

The specified distribution groups, mail-enabled security groups, or Microsoft 365 Groups in your organization.



### Domains

All recipients in the specified accepted domains in your organization.

Microsoft 365 Defender

Policies & rules > Threat policies > Create anti-spam inbound policy

- ✓ Name your policy
- **Users, groups, and domains**
- Bulk email threshold & spam properties
- Actions
- Allow & block list
- Review

## Users, groups, and domains

Add users, groups and domains to include or exclude in this policy.

**Include these users, groups and domains**

Users

all

Suggested contacts

All Company

Exclude these users, groups and domains

Click in the appropriate box, start typing a value [in the example above, we typed All] and select the value that you want from the results. Repeat this process as many times as necessary. To remove an existing value, click remove next to the value.

For users or groups, you can use most identifiers (name, display name, alias, email address, account name, etc.)

When you're finished, click **Next**.



On the **Bulk email threshold & spam** properties page that appears, configure the following settings:

**Bulk email threshold:** Specifies the bulk complaint level (BCL) – BCL can be set from 1 to 9. A lower value indicates benign bulk email (newsletters, ads you signed up for, mail from known good bulk senders, etc.). A higher value indicates the bulk message is 'bad' (likely unwanted and more likely to resemble spam or spam-like).

The recommend default value is 7.

The screenshot shows the Microsoft 365 Defender interface for configuring an anti-spam inbound policy. The navigation pane on the left includes steps: Name your policy, Users, groups, and domains, Bulk email threshold & spam properties (highlighted), Actions, Allow & block list, and Review. The main content area is titled 'Bulk email threshold & spam properties' and contains the following settings:

- Bulk email threshold:** A slider set to 7 (Recommended default). A note states: "A higher bulk email threshold means more bulk email will be delivered".
- Spam properties:**
  - Increase spam score:** Specify whether to increase the spam score for messages that include these types of links or URLs.
  - Mark as spam:** Specify whether to mark messages that include these properties as spam.
- Test mode:** Configure the test mode options for when a match is made to a test-enabled advanced option.
  - None
  - Add default X-header text
  - Send Bcc message

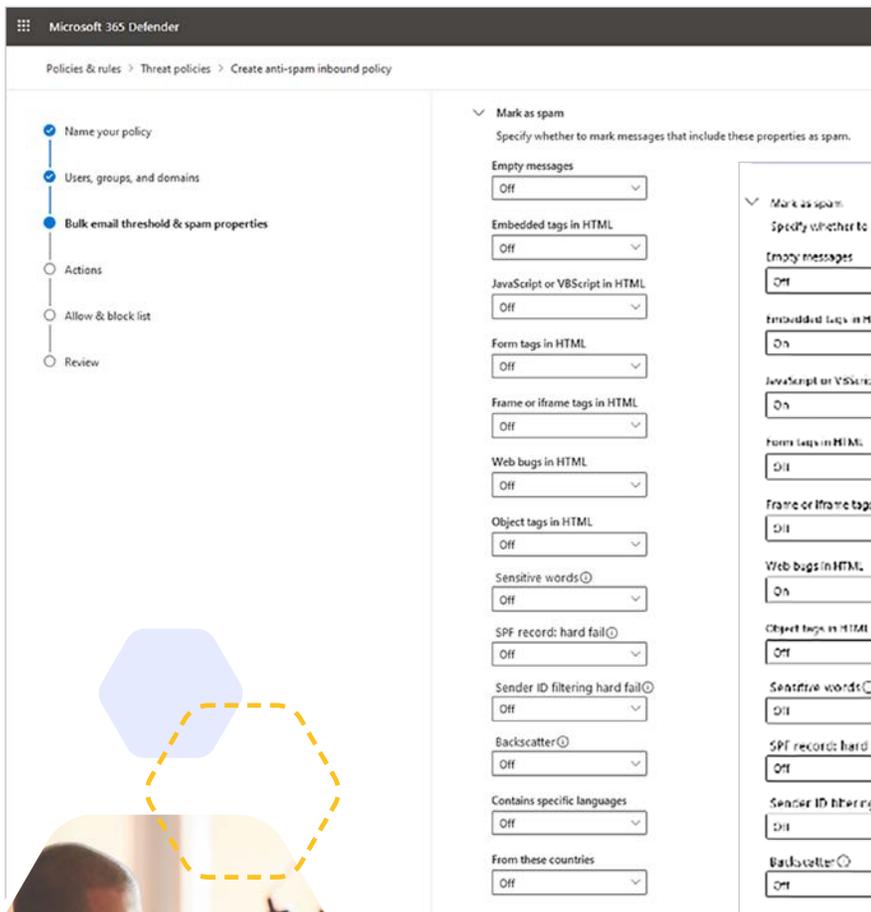
**Increase spam score and Mark as spam\*:** Contains the Advanced Spam Filter (ASF) settings that are turned off by default.

- ASF settings are in the process of being deprecated, and their functionality is being incorporated into other parts of the filtering stack. We recommend that you leave all of these ASF settings turned off in your anti-spam policies.

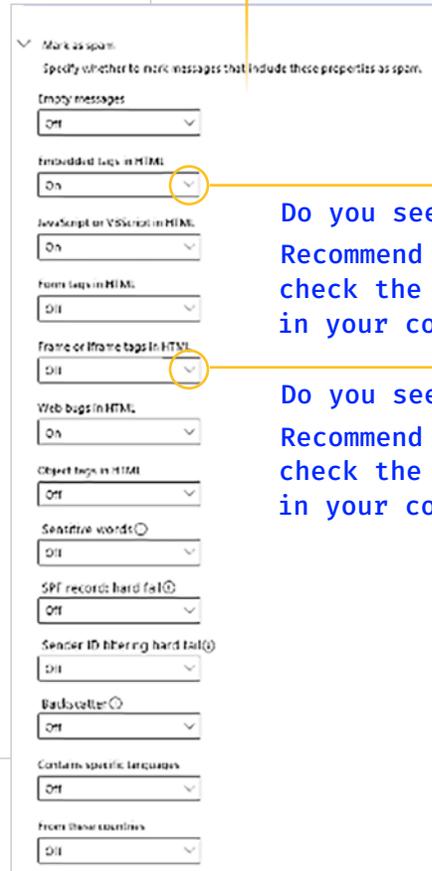
**Our recommendation to set as 1st review**

**Increase spam score settings:** The following ASF settings set the spam confidence level (SCL) of detected messages to 5 or 6, which corresponds to the **Spam** filter verdict and the corresponding action in anti-spam policies.

Anti-spam Policy Setting	Description	Recommended Value
Image links to remote websites	Messages that contain <img> HTML tag links to remote sites (for example, using http) are marked as spam.	ON
Numeric IP address in URL	Messages that contain numeric-based URLs (typically, IP addresses) are marked as spam.	ON
URL redirect to other port	Message that contains hyperlinks that redirect to TCP ports other than 80 (HTTP), 8080 (alternate HTTP), or 443 (HTTPS) are marked as spam.	ON
Links to .biz or .info websites	Messages that contain .biz or .info links in the body of the message are marked as spam.	OFF



Our recommendation to set as 1st review



Do you see a lot of cases? Recommend ON but check the usage of this in your company?

Do you see a lot of cases? Recommend off but check the usage of this in your company?

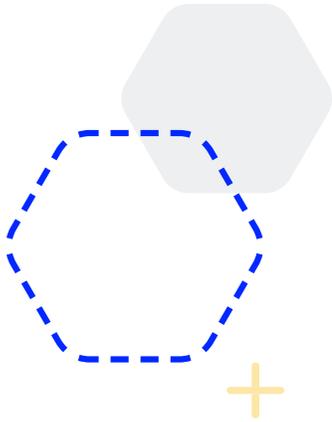


**Mark as spam settings:** The following ASF settings set the SCL of detected messages to 9, which corresponds to the **High confidence spam** filter verdict and the corresponding action in anti-spam policies.

Anti-spam Policy Setting	Description	Recommended Value
Empty messages	Messages with no subject, no content in the message body, and no attachments are marked as high confidence spam.	<b>OFF</b>
Embedded tags in HTML	<p>Message that contains &lt;embed&gt; HTML tags are marked as high confidence spam.</p> <p>This tag allows the embedding of different kinds of documents in an HTML document (for example, sounds, videos, or pictures).</p>	Do you see a lot of cases? Recommend <b>ON</b> but check the usage of this in your company?
JavaScript or VBScript in HTML	<p>Messages that use JavaScript or Visual Basic Script Edition in HTML are marked as high confidence spam.</p> <p>These scripting languages are used in email messages to cause specific actions to automatically occur.</p>	<b>ON</b>
Form tags in HTML	<p>Messages that contain &lt;form&gt; HTML tags are marked as high confidence spam.</p> <p>This tag is used to create website forms. Email advertisements often include this tag to solicit information from the recipient.</p>	<b>OFF</b>
Frame or iframe tags in HTML	<p>Messages that contain &lt;frame&gt; or &lt;iframe&gt; HTML tags are marked as high confidence spam.</p> <p>These tags are used in email messages to format the page for displaying text or graphics.</p>	Do you see a lot of cases? Recommend <b>OFF</b> but check the usage of this in your company?
Web bugs in HTML	<p>A web bug (also known as a web beacon) is a graphic element (often as small as one pixel by one pixel) that's used in email messages to determine whether the message was read by the recipient.</p> <p>Messages that contain web bugs are marked as high confidence spam.</p> <p>Legitimate newsletters might use web bugs, although many consider this an invasion of privacy.</p>	<b>ON</b>

Anti-spam Policy Setting	Description	Recommended Value
Object tags in HTML	<p>Messages that contain &lt;object&gt; HTML tags are marked as high confidence spam.</p> <p>This tag allows plug-ins or applications to run in an HTML window.</p>	OFF
Sensitive words	<p>Microsoft maintains a dynamic but non-editable list of words that are associated with potentially offensive messages.</p> <p>Messages that contain words from the sensitive word list in the subject or message body are marked as high confidence spam.</p>	OFF
SPF record: hard fail	<p>Messages sent from an IP address that isn't specified in the SPF Sender Policy Framework (SPF) record in DNS for the source email domain are marked as high confidence spam.</p>	OFF
Sender ID filtering hard fail	<p>Messages that hard fail a conditional Sender ID check are marked as spam.</p> <p>This setting combines an SPF check with a Sender ID check to help protect against message headers that contain forged senders.</p>	OFF
Backscatter	<p>Backscatter is useless non-delivery reports (also known as NDRs or bounce messages) caused by forged senders in email messages.</p>	OFF





\*Contains specific languages and from these countries are not part of ASF settings.

**Contains specific languages**

On

**From these countries**

On

- **Contains specific languages:** Click the box and select **On** or **Off** from the drop-down list. If you turn it on, a box appears. Start typing the name of a language in the box. A filtered list of supported languages will appear. When you find the language that you're looking for, select it. Repeat this step as many times as necessary. To remove an existing value, click **remove** next to the value.
- **From these countries\*:** Click the box and select **On** or **Off** from the drop-down list. If you turn it on, a box appears. Start typing the name of a country in the box. A filtered list of supported countries will appear. When you find the country that you're looking for, select it. Repeat this step as many times as necessary. To remove an existing value, click **remove** next to the value.

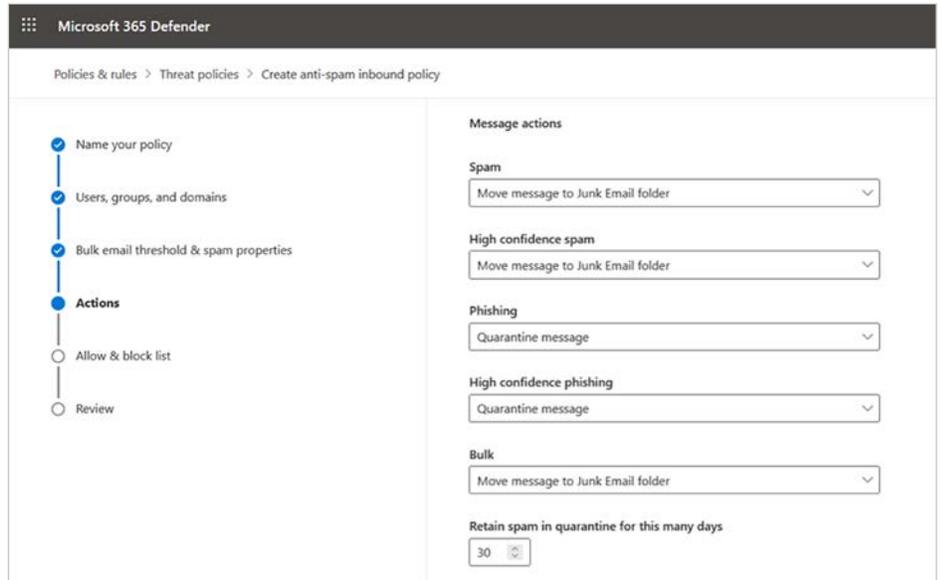
When you are finished, click **Next**.

5

On the **Actions** page that appears, configure the following settings:

**Message actions:** Select or review the action to take on messages based on the following spam filtering verdicts:

- Spam
- High confidence spam
- Bulk



The **available actions for spam filtering** verdicts are described in the table below:

- ✓ A check mark indicates the action is available (not all actions are available for all verdicts).
- \* An asterisk after the check mark indicates the default action for the spam filtering verdict.

Action	Spam	High Confidence Spam	Bulk
<b>Move message to Junk Email folder:</b> The message is delivered to the mailbox and moved to the Junk Email folder. <sup>1</sup>	✓*	✓*	✓*
<b>Add X-header:</b> Adds an X-header to the message header and delivers the message to the mailbox. You enter the X-header field name (not the value) later in the <b>Add this X-header text box</b> . For <b>Spam</b> and <b>High confidence spam</b> verdicts, the message is moved to the Junk Email folder. <sup>1,2</sup>	✓	✓	✓*
<b>Prepend subject line with text:</b> Adds text to the beginning of the message's subject line. The message is delivered to the mailbox and moved to the Junk email folder. <sup>1,2</sup> You enter the text later in the <b>Prefix subject line with this text box</b> .	✓	✓	✓
<b>Redirect message to email address:</b> Sends the message to other recipients instead of the intended recipients. You specify the recipients later in the <b>Redirect to this email address box</b> .	✓	✓	✓
<b>Delete message:</b> Silently deletes the entire message, including all attachments.	✓	✓	✓
<b>Quarantine message:</b> Sends the message to quarantine instead of the intended recipients. You specify how long the message should be held in quarantine later in the <b>Quarantine box</b> .	✓	✓	✓
<b>No action</b>			✓

<sup>1</sup> In Exchange Online, the message is moved to the Junk Email folder if the junk email rule is enabled on the mailbox (it's enabled by default).

In hybrid environments where EOP protects on-premises Exchange mailboxes, you need to configure mail flow rules (also known as transport rules) in on-premises Exchange to translate the EOP spam filtering verdict so the junk email rule can move the message to the Junk Email folder.

<sup>2</sup> You can this use value as a condition in mail flow rules to filter or route the message.



- **Retain spam in quarantine for this many days:** Specifies how long to keep the message in quarantine if you selected **Quarantine message** as the action for a spam filtering verdict. After the time period expires, the message is deleted.
- **Add this X-header text:** This box is required and available only if you selected **Add X-header** as the action for a spam filtering verdict. The value you specify is the header field name that's added to the message header. The header field value is always This message appears to be spam.
- **Prepend subject line with this text:** This box is required and available only if you selected **Prepend subject line with text** as the action for a spam filtering verdict. Enter the text to add to the beginning of the message's subject line.
- **Redirect to this email address:** This box is required and available only if you selected the **Redirect message to email address** as the action for a spam filtering verdict. Enter the email address where you want to deliver the message. You can enter multiple values separated by semicolons (;).
- **Enable safety Tips:** By default, Safety Tips are enabled, but you can disable them by clearing the checkbox. For more information about Safety Tips, see [Safety Tips, see Safety tips in email messages](#).
- **Enable end-user spam notifications:** For more information, see the [Configure end-user spam notifications](#) section later in this topic.

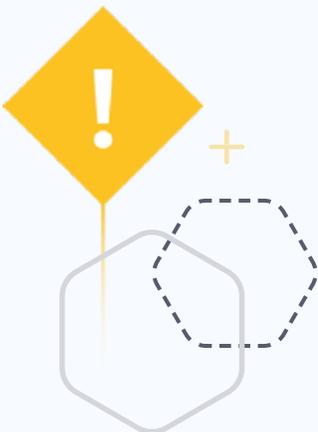
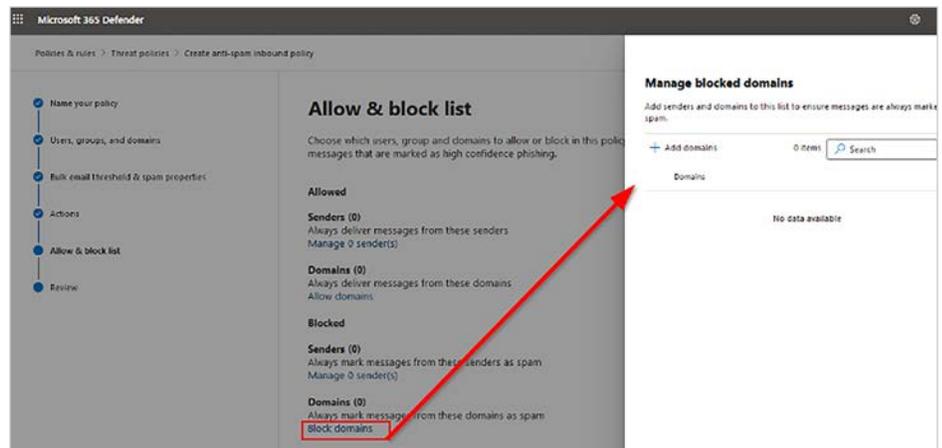
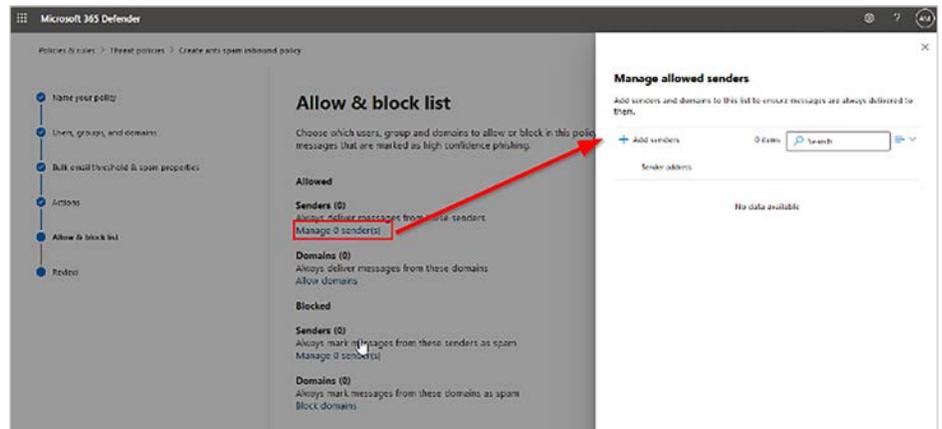
When you're finished, click **Next**.

The screenshot shows the Microsoft 365 Defender interface. The breadcrumb trail is: Policies & rules > Threat policies > Create anti-spam inbound policy. On the left, a navigation pane shows the configuration steps: Name your policy, Users, groups, and domains, Bulk email threshold & spam properties, Actions, Allow & block list (highlighted), and Review. The main content area is titled 'Allow & block list' and includes a note: 'Choose which users, group and domains to allow or block in this policy. Note: The allow entries that you configure here do not apply to messages that are marked as high confidence phishing.' Below this, there are sections for 'Allowed' and 'Blocked' entries, each with 'Senders (0)' and 'Domains (0)' sub-sections, and links to 'Manage 0 sender(s)' or 'Block domains'.



On the **Allow & block list** flyout that appears, you can configure message senders by email address or email domain that are allowed to skip spam filtering.

In the **Allowed** section, you can configure allowed senders and allowed domains. In the **Blocked** section, you can add blocked senders and blocked domains.



## IMPORTANT

Think very carefully before you add domains to the allowed domains list.

Never add your own accepted domains or common domains (for example, microsoft.com or office.com) to the allowed domains list. If these domains are allowed to bypass spam filtering, allow attackers an easily send email into your organization.

Manually blocking domains by adding the domains to the blocked domains list isn't dangerous, but it can increase your administrative workload. For more information, see [Create block sender lists in EOP](#).

On the confirmation page that appears, click **Done**.

## Wrapping Up

### Reporting

There are several Microsoft reports that will assist in monitoring the progress of this Spam Tuning.

Office 365 spam detection report is user to identify inbound and outbound spam emails that are filtered by Exchange Online Protection (EOP) and anti-spam technologies. In the O365 Security and Compliance center, go to 'Reports' and see the 'Dashboard'. In the dashboard, see 'Spam Detections'. On clicking each report, you will find the email details. But it doesn't have a filter to identify sent and received emails separately

### SPF/DKIM/DMARC

Finally, IRONSCALES recommends configuring SPF, DKIM, and DMARC if possible, within your organization as these controls will reduce the amount of Spam your Company receives. These controls are not a trivial implement but will be worth the effort to implement.



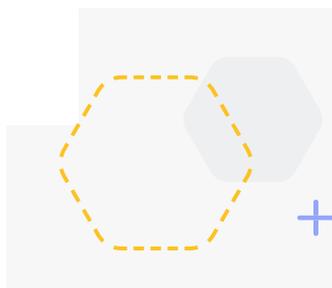
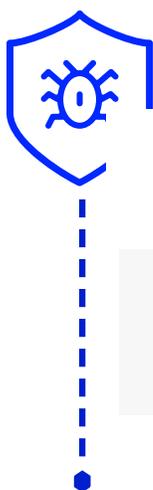
[SPF](#)



[DKIM](#)

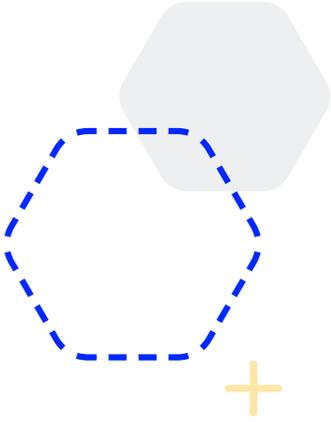


[DMARC](#)



**Congrats – you did it!** Now that you have completed the Microsoft EOP anti-spam configuration work you are ready to get started with part two: Turning on your IRONSCALES service.

IRONSCALES' advanced anti-phishing platform is natively integrated with Office 365 email service, protecting your organization's mailboxes across all devices, operating systems and networks. Using the O365 integration, IRONSCALES automatically detects and mitigates email phishing attacks in real-time, with or without human intervention, followed by an enterprise-wide remediation response. The automated phishing response technology is intelligent enough to analyze the maliciousness of the threat and remove it from all employee inboxes to prevent it from spreading – all of which alleviates the burden on the SOC team. With IRONSCALES AI-Powered Incident Response, each time a malicious event is detected, it remembers it so that the same type of attack can never successfully infiltrate any other computer within its network again.

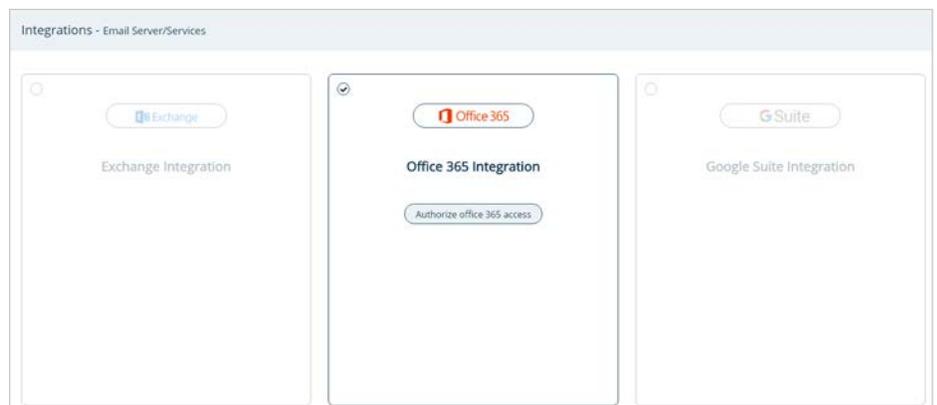


## Prerequisites

- Office 365 global admin user account access
- Users' information:
  - Protected mailboxes must be uploaded to the Profiles Management page on our dashboard
  - The uploaded profiles/mailboxes must be in an active state on the Profiles Management page
  - Mailbox userType in the O365 settings must show as a member (guests will not be synced)

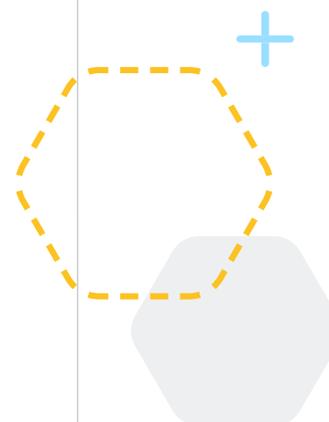
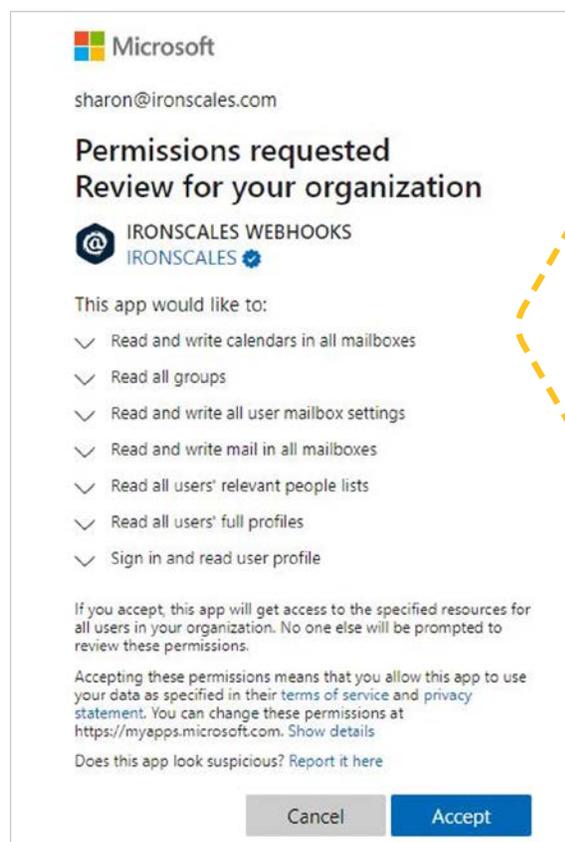
## Office 365 Integration

- Go to [Email Server Settings](#) > Click Office 365 Integration > Authorize Office 365 access



You will be redirected to the Microsoft login page.

Log in with your Office 365 global admin account > Click Accept to grant the IRONSCALES application the required permissions:



- Choose what steps you would like IRONSCALES to complete automatically for you:
  - This option will only appear upon Office 365 integration. If your integration is already active. You will need to disable and re-enable it to have that option available.
- Sync my mailboxes automatically using 'Auto-Sync' and install the report button in my company's mailboxes: This option will allow IRONSCALES to [upload/sync](#) all your Office 365 users into the [Protected Mailboxes](#) page and it will distribute the [OWA Report as Phishing](#) button to all your Office 365 users automatically.
  - You will be required to use an "[Exchange admin](#)" user to allow IRONSCALES to distribute the reporting button. IRONSCALES will not store your credentials. You may change the user's password once the deployment has been confirmed, or create a dedicated user with Powershell permissions for this matter.

- Sync my mailboxes automatically using 'Auto-Sync': This option will allow IRONSCALES to [upload/sync](#) all your O365 users into the [Protected Mailboxes](#) page. You will need to distribute the report as a phishing button manually through your Office 365 Admin Center, following the [OWA Report as a Phishing](#) article.

- I will sync my mailboxes manually: IRONSCALES will not do any additional integrations on your dashboard. You will need to [Upload / Sync](#) Mailboxes to your dashboard and to distribute the report as a phishing button manually through your Office 365 Admin Center, following the [OWA Report as Phishing](#) Button article.
- [Will show only when choosing option 1 or 2 in the previous step] Choose which groups you would like IRONSCALES to sync with your Office 365 account or check "Sync all users" to sync all Office 365 enabled users into the IRONSCALES Protected Mailboxes list.
  - All relevant groups discovered in your Office 365 account will be synced to IRONSCALES
  - New groups in Office 365 may take up to 5 minutes to sync into the IRONSCALES system
- Once the integration process is complete, you will get an email with the status of the automatic deployment. If any of these steps fail, you will receive a link with instructions on how to manually complete your integration.

Your IRONSCALES + Office 365 integration is ready! Please note that it can take up to one hour for the full synchronization process.



To learn more about how to get started, [request a demo today](#)



IRONSCALES is a self-learning email security platform that can predict, detect and respond to email threats within seconds.

Email threats are growing exponentially and morphing at scale. Each day, billions of new, increasingly sophisticated phishing attacks are launched globally. Legacy technologies like security email gateways (SEGs) have been shown to allow up to 25% of incoming phishing attacks through to their intended targets.

With IRONSCALES, you and your organization are Safer Together because of the following:

- Advanced malware/URL protection
- Mailbox-level Business Email Compromise (BEC) protection
- AI-powered Incident Response
- Democratized real-time threat detection
- A virtual security analyst
- Gamified, personalized simulation and training

To learn more, please visit [www.ironscALES.com](http://www.ironscALES.com) today!

